LETHBRIDGE PRIMARY SCHOOL

E-SAFETY POLICY

Reviewed: April 2021	Next review: April 2023

Lethbridge Primary School is committed to providing a safe and secure environment for pupils, staff and visitors and promoting a climate where pupils and adults feel confident about sharing any concerns that they may have about their own safety or the wellbeing of others.

This policy should be read and implemented in conjunction with the child protection policy, anti-bullying policy, behaviour policy and data protection policy.

1. Curriculum

- A planned e-safety curriculum is provided as part of Computing and PHSE. Curriculum information can be found at: https://lethbridgeschool.org.uk/curriculumComputing.php
- Key e-safety messages are reinforced through our school website, assemblies and classroom activities.
- Children are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Children are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Children are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies the internet and mobile devices
- Internet use in lessons is pre-planned, following best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

2. Parent and Carers

Parents and carers play an essential role in the education of their children and in the monitoring of the children's on-line behaviours. It is the responsibility of parents and carers to:

a) Read the AUP and encourage their children to adhere to the guidelines.
b) Support the school in their e-safety approaches by discussing e-safety issues with their children and reinforce appropriate, safe online behaviours at home.

c) Role model safe and appropriate use of technology and social media.
d) Abide by the school's AUP and identify changes in behaviour that could indicate that their child is at risk of harm online.
e) Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
f) Use school systems, such as learning platforms, and other network resources, safely and appropriately.
g) Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

The school will seek to provide information and awareness to parents and carers through:

- Letters, newsletters and the school website
- Online safety parent information events and online workshops
- Reference to the relevant web sites and publications eg *www.swgfl.org.uk* *www.saferinternet.org.uk/* *http://www.childnet.com/parents-and-carers*

3. Technical – infrastructure / equipment, filtering and monitoring

- Internet Filtering is provided by Surf Protect http://www/surfprotect.co.uk
- We will work in partnership with parents, the LA, DfE and the Internet Service Provider - Exa Networks Ltd http://www.exa.net.uk to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider. Children will be educated as to the correct and safe procedure to do this.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Any material that the school believes is illegal must be referred to the Internet Service Provider.
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate.
- The school has provided enhanced / differentiated user-level filtering
- An agreed policy is in place regarding the extent of personal use that users staff and their family members are allowed on school devices that may be used out of school.

4. Use of digital and video images

The school will gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.

- When using digital images, staff should inform and educate children about the risks associated with the taking, using, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. They are taught about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. Pupils are advised about the need to keep their data secure and what to do if they are subject to bullying or abuse
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.

5. Data Protection

Please see data protection policy.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected

- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

6. Internet Use

The school has a duty to provide children with quality internet access as part of their learning experience. Pupils use the internet widely outside of school and need to learn to evaluate internet information and to take care of their own safety and security.

- The school's internet access will be designed to enhance and extend education.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Access levels to the internet will be reviewed to reflect the curriculum, requirement and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet materials in their own work.

7. Monitoring and review

The Computing subject leader provides an annual Action Plan in which s/he evaluates the strengths and weaknesses in the subject, plans for further implementations and projects using Computing and indicates areas for further improvement. The Computing Subject leader attends Network meetings to stay updated in developments within Computing.

8. Use of Personal Devices and Mobile Phones

Mobile phones brought into school are entirely at the staff member's, pupil's & parents/carers' or visitor's own risk. The School accepts no responsibility for the loss, theft or damage of any mobile phone or personal device brought into school.

The use of personal mobile phones or cameras by pupils or staff is not permitted at any time when pupils are present. The only exception to this is the use of a mobile phone to make calls during an emergency. Mobile phones are also used by teachers to enable access to CPOMS.

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as child protection, data protection and AUPs.

Staff are advised to:
a) Keep mobile phones and personal devices in a safe and secure place during lesson time.
b) Keep mobile phones and personal devices switched off or switched to 'silent 'mode during lesson times.
c) Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
d) Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones for contacting pupils or parents and carers.
Staff will not use personal devices, such as mobile phones, watches, tablets or cameras:
a) To take photos or videos of pupils and will only use work-provided equipment for this purpose.
b) Directly with pupils, and will only use work-provided equipment during lessons/educational activities.

Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents/carers, then a school phone will be provided and used, unless they have the prior permission of the head-teacher. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

9. Official Use of Social Media

The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
a) The official use of social media as a communication tool has been approved by the Headteacher.
b) Leadership staff have access to account information and login details for the social media accounts, in case of emergency, such as staff absence.

Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
a) Staff use school provided email addresses to register for and manage any official school social media channels.
b) Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
c) Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including: anti-bullying, child protection and data protection.
a) All communication on official social media platforms will be clear, transparent and open to scrutiny. The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

10. School Procedures

All pupils, members of staff and other adults have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that all users are fully aware of their responsibilities when using technology, they are required to read and sign the appropriate acceptable use policy.

In the event of an e-safety incident involving illegal activity, the school will:
a) Inform a member of the safeguarding team for incidents involving pupils, and inform the Principal/Headteacher for incidents involving staff.
b) Secure and preserve all evidence and hardware.
c) The head teacher will report the incident to the appropriate agencies, such as IWF, the Police or CEOP.
d) Take internal action through the school's behaviour, anti-bullying and child protection policies, as appropriate.

E-safety incidents that involve inappropriate rather than illegal activity will be dealt with through the school's behaviour, anti-bullying and child protection policies, as appropriate. A log of all reported e-safety incidents related to children will be maintained on CPOMs.